Setting up and securing your wireless network

How to guide

What does it take to go wireless?

Creating a wireless network may seem daunting initially, but it's something that you can do and do successfully. This guide will give you the basics of how to set up and secure your Wireless Local Area Network (WLAN). You'll need some good planning, the right equipment, and a little bit of patience.

Get un-wired

Going wireless might be one of the smartest things you can do for your growing business. It's less expensive and less invasive than creating a traditional wired network—there's no need to invest in cables or drill holes in walls—and it's certainly less cluttered. But creating your own wireless network means more than saving some money and getting rid of cables and wires. A wireless network means more freedom.

In a wired office, work gets done when employees sit at their desks. When you go wireless, your employees can work anywhere—in conference rooms, lunchrooms, a coworker's office. It makes for a more accommodating, more collaborative atmosphere. With a wireless network, you can expect more productivity in your workplace.

What is a WLAN?

On the most basic level, a WLAN, or Wireless Local Area Network, is a series of devices—access points or routers and Wi-Fi radios—that connect to one another and transmit data via radio signals. Access points are base stations that connect users to each other, to your server(s), and to the Internet. They're best for wireless networks with more than just a few users. Routers are more appropriate for very small wireless networks and perform the duties of both an access point and a server. If you're building a wireless network for more than four or five users, you'll likely want to use access points. Wi-Fi radios are usually built into your computer's hardware (and if one isn't built in, it can be added).

Table of contents

1 plan

1 Planning for your wireless network

Planning for your wireless network

Determine your needs—budget, time, and assistance

Before you start building your wireless network, you need to take stock. Following are a few questions and tips to help you determine your needs.

1 plan

1. How many users will your wireless network service, and what will those users be doing?

Typically, you'll need one access point for every 15 to 20 users. So if you have 100 users, count on purchasing at least five access points. Then you need to consider how they'll be using the wireless network in order to determine which wireless standard to support. If those users are simply sharing Internet access, 802.11b is your best bet. If they're transferring hefty files, you might need 802.11a or 802.11g. Take a look at the wireless standard table for more information on the benefits and drawbacks of each standard.

Wireless standard	Data rate	Benefits	Drawbacks
802.11b	11 Mbps on 2,4GHz frequency	Good for sharing an Internet connection. Good for large coverage areas. Currently the most widespread standard supported.	Not good for moving large files.
802.11g	54 Mbps on 2,4GHz frequency	Very good for moving large files. Backward-compatible with 802.11b.	Shorter range. More susceptible to interference.
802.11a	54 Mbps on 5Ghz frequency	Very good for moving large files. Runs on 5Ghz frequency, so experiences less radio interference than 802.11b/g.	Shorter range. Not backward-compatible with 802.11b.

2. How much can you afford to spend?

Of course, it would be wonderful to make every part of your workplace wireless, but your budget may not allow it. So take a realistic look at what you have to spend. Later, after you've identified your needs and assessed your space, you'll know how much equipment you need to buy. Then, if necessary, you can adjust your wireless network plan to fit within your budget.

3. Can you do it yourself or do you need help?

Are you or someone in your organization comfortable enough with technology to do the job? And, just as importantly, do you have the time? If the answer to either question is "No," then you'll need to outsource. Whether you outsource the entire job or just a part of it, being an informed client is key to a successful project. So be sure to learn about the process even if you're not going to do it yourself.

Part	Price Range
Router	$50–$150
Access point	$130–$600
Wi-Fi radio PC card	$20–$100
Antenna	$25–$200
Ethernet cable (25 ft.)	$5–$25
Power surge protector	$10–$100

4. Down the road, what do you want your wireless network to look like?

Will your business be growing? Will your technological needs change? Will your workspace change? Anticipating your future may affect your choice of equipment and how you arrange your wireless network. For example, if you know that you're going to need more bandwidth down the road, you might invest in access points that you can upgrade from 802.11b to 802.11g.

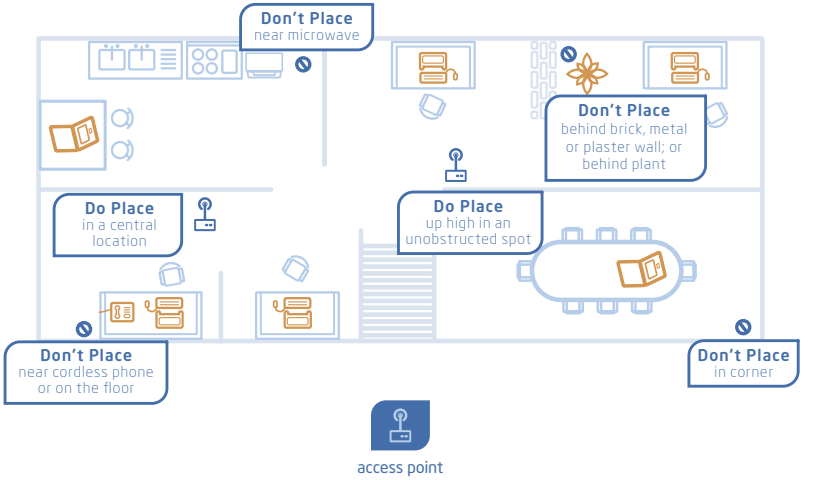
1 plan

Assess your space

Once you've identified your needs, it's time to assess your space and do a site survey. The complexity of your site survey will depend on the complexity of your proposed wireless network and the makeup of your space. But here are the basics you'll need to consider:

- The physical space. Look for any obstacles that can interfere with radio frequency. Probable culprits are metal (in doors, air conditioning units, etc.), microwaves, and cordless phones—or objects like large trees if you're including outside spaces. You should also note power outlets, because their placement dictates, in part, where your access points can be.

Where to place access points



- Your existing network. If you have one, you'll need to make sure that your new wireless network is compatible. What operating systems do your current users have? You may need to do some updating in order to make their laptops and desktops Wi-Fi compatible. And be sure to give all new devices, servers, and networks unique names so that there's no overlap with your existing naming system. You'll also need to think about the kind of use your existing network gets—sharing Internet access, transferring large data, etc.—to help you determine which wireless standard to support.

- Coverage and range. The most crucial part of planning a wireless network is testing the signal strength in the various areas of your workplace. To do this, you'll create a mock wireless network. Set up an access point (you can use a laptop computer) in a spot where you might want an access point. This will act as your transmitter. Then use a laptop with site survey software as the mobile receiver. Test the signal strength and note it on a map of your site. Continue to move your access point and test until you've covered your entire space.

As you conduct your survey, be sure to document the results. This will help down the line should you ever need to do some maintenance work or you come up against a wireless network problem.

Identify your access points

If you've done a thorough site survey, deciding where to place your access points will be a snap. A few rules of thumb to make the task easier:

- Access points in an unobstructed office setting usually have a range of 150–300 feet.
- Individual access point ranges should overlap to give users continuous coverage.
- Position your access points off the ground and away from obstacles that might cause interference.
- If you're using two antennas, position one vertically and one horizontally for maximum coverage.

To learn more: www.intel.com/business/smallbusiness/wireless/.

1 plan

2

Implementing your wireless network

Implementing your wireless network

Equipment and supplies

The list of equipment you'll need to set up your wireless network is refreshingly short. But though there are only a few items on the list, how many of each component you'll need will depend on the size of your wireless network.

The equipment list

- A transmitter and a receiver to conduct the site survey—This can be two laptops or one laptop and a router or access point.
- Site survey software—This can range in price from the free utility included with your PC card to all-inclusive kits that can cost $5,000 or more.
- Wi-FI radios—Each of your wireless network's clients (users) needs to have one. It may be already installed as part of your PC card. If not, for PC users you can buy PC cards or wireless USB adapters; for Mac* users, AirPort cards.
- Access points—There are many different brands of access points on the market. We recommend buying all your access points from the same manufacturer, or else be sure to check for interoperability.
- Antennas—Access points usually come with one, but you may find during the site survey that you need additional antennas for better reception in certain areas.
- Ethernet cable—You'll need this to connect your access points to the Internet.

Setup—access points

Before you get started, it's always a good idea to read the instructions included with the equipment you've purchased. Once you've done that, you're ready to go. Connecting your access point is as simple as attaching the antennas to the device, connecting it to your computer with an Ethernet cable, and plugging it into a power source.

Once you've connected your access point, you'll need to configure it. If you've purchased a new access point, it likely came with a web-based interface or desktop software utility that will walk you through the configuration process. The process differs slightly from manufacturer to manufacturer, but these are the basic steps:

1. Select AP mode—You may need to tell your device to act as an access point. If so, choose AP mode at the appropriate prompt.
2. Change the default SSID—It's important that you change your device's default SSID,

or Service Set ID, to protect your wireless network. When you do this, be sure to choose something that will be difficult for intruders to guess. Use both numbers and letters, and use the maximum number of characters allowed (or something close to it).

3. Set the channel—You need to select the channel you'll use to communicate with your access point. Channel 6 may be the default. If you have several access points in close proximity to one another, you may want to use a different channel to reduce interference.
4. Activate security measures—We cover this crucial step later in this guide.

Note: You need to follow these steps for each of your access points.

Setup—client side

Before configuring your client-side operating system, you need to ensure that you have the necessary hardware and that it is properly installed. In other words, you need to have a PC card or some comparable Wi-Fi-ready hardware installed. Assuming that you do, configuring your operating system is fairly straightforward.

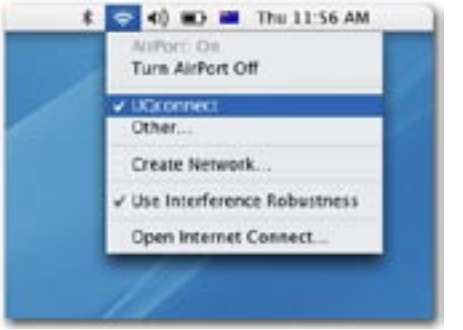
Microsoft Windows XP*

Because XP is designed to accommodate wireless networks, you may not have to do anything to configure your OS. Try mousing over the wireless network icon on your desktop (it's probably at the bottom right with the other icons). If you get a popup with your wireless network named showing that you're connected, you're all set. If not, right click the icon and choose View Available Wireless Networks from the menu. A new, large popup will appear and your wireless network SSID name should now show up. Choose it and click Connect.

Mac OS X

Like Windows XP, Mac OS X is ready for wireless networking. You may find that you don't have to do a thing to get connected—that you're automatically connected. But if you're trying to connect with a protected access point, use the AirPort menu (at the top right on your monitor), select the wireless network you want, enter any necessary passwords, and click OK. If you don't see your wireless network on the list, choose Other, enter your SSID and any necessary passwords, and click OK.

See www. linux.org to set up Linux systems.



implement

3

Securing your wireless network

Securing your wireless network

You're almost ready to launch your wireless network, but before you do, you need to protect it. WLANs are susceptible to a variety of security breaches—unauthorized access, eavesdropping, rogue access points—but with a few simple precautions, you can better protect your wireless network.

Basic security measures

- Change your access point default settings. Your access point comes with default settings in place—in particular, the SSID. Changing the default SSID is a simple yet critical way to protect your wireless network.
- Disable SSID broadcasting. You can opt to do this when you configure your access point. When you disable SSID broadcasting, your wireless network name is no longer visible, requiring users to know the SSID in order to access the wireless network.
- Add a firewall. Adding a firewall can be as simple as installing basic firewall software, and it's your first line of defense against unwanted users.
- Use virus-scanning software. You probably already do this, but if you don't, make it a mandatory practice in your workplace. It's the easiest way for individual users to protect their data and to determine whether or not security has been breached.

Advanced security measures

- WEP vs. WPA and WPA2

  Wired equivalent privacy (WEP) was the first kind of security available for wireless networks. It uses an encryption key to scramble data as it's transferred from clients to access points. It's not foolproof, as it's susceptible to more determined hackers, but it may provide enough security for smaller businesses. WPA, or Wi-Fi Protected Access, is the next generation of WEP. It uses a more advanced authentication and encryption process for a more secure wireless network. WPA2 is an even more powerful version of WPA. To implement WPA or WPA2, you'll need to update your access points and client programs. Check with your access point and OS vendors for WPA updates that you can upload and install on your devices.

- Virtual Private Networks (VPNs)

  VPNs use public networks, like the Internet, to allow a user on an insecure network to safely access information on a secure wireless network. They create a virtual, encrypted tunnel where information passes between a user and the private wireless network without the threat of security breaches. VPNs are a great way to protect your wireless network and still allow employees to work remotely. You will need an experienced IT professional to configure a VPN for your business.

Test and go live

Test your wireless network before officially going live. There are many variables to be tested, and some are quite complex. Your first focus should be on signal strength and areas of interference. If you have strong signal strength and are able to upload and download large files with reasonable throughput, you are in great shape. If you are not satisfied with your wireless network performance, you may seek professional advice, because fine-tuning a WLAN can involve complex tasks.

To learn more: www.intel.com/business/smallbusiness/wireless.

Enjoy your wireless network

Congratulations—you've done it. You've planned, implemented, and secured your wireless network. Now you get to enjoy it. Keep in mind that your wireless network will likely evolve over time. To keep it running smoothly, make sure that you keep your security measures up to date and that your users know what your security protocols are.

Troubleshooting

No matter how meticulous you are in setting up your WLAN, there's always a chance that you'll come up against an obstacle. Don't worry. Most of the problems you'll experience with your wireless network are common and relatively easy to solve. Here are a few pointers to guide you in your troubleshooting:

Identify the problem

Before you can fix it, you have to know what it is. Are you having a device issue? An interference problem? A security breach? Start the process by trying to identify the source of the problem. This is where your site survey documentation will come in handy. Use it as your roadmap in the process of elimination. If your wireless network is complex enough and you can't identify the problem, you might consider retaining the services of an IT network professional to help you isolate the issue.

Before you do anything else...try the simplest solutions

Network problems are often as simple as an unplugged cable. Before you start thinking about radio frequencies and interoperability, ask yourself (and answer) these simple questions:

1. Are there any unplugged components?
2. Are there any loose cables?
3. Is any wireless network equipment damaged or broken?
4. Is there anything new in our workplace that may be causing interference?
5. Have we added new users who are taxing our bandwidth?
6. Are we transferring heftier information and taxing bandwidth?
7. Is the problem associated with an area of the wireless network that has a weak signal?
8. Was there a recent loss of power, and the hardware needs to be reset?
9. Is it a server issue or a broadband issue and not a wireless network issue?

Check the basics

So it's not as simple as an unplugged device. Your next move should be to check connectivity and compatibility. Make sure that all components are connected to the wireless network. Also check that devices are using compatible standards and the same channel. Have you added any new devices to your wireless network? You may be experiencing interoperability issues.

Confirm that your information is correct

When all else fails, it's time to get nitpicky. Check to see that network addresses, SSIDs, and WPA configurations are correct. This can be tedious, as you may have to go device by device to check SSIDs, but it might also solve your problem.

Still haven't found the solution? Visit www.intel.com/business/smallbusiness/wireless/ for more in-depth troubleshooting.

Key terms

802.11a/b/g—These numbers and letters refer to the standard used to describe bandwidth, that is, the speed at which information is transferred between access points and users. For more information on wireless standards, refer to our wireless standard table.

PC Card—PC Cards, or PCMCIA cards (from Personal Computer Memory Card International Association) are small devices that can be installed in a laptop to give that computer wireless capability.

Service Set ID (SSID)—A sequence of letters or numbers representing the name of a wireless local area network. The SSID is broadcast to all wireless devices within range of the wireless network access point.

Site survey software—The software you need to have on the laptop you use as a mobile receiver. Site survey software can be a simple as the utility that comes with your PC card or as complex as the comprehensive kits sold by third-party vendors.

Maximizing your wireless network with Intel® Centrino® Duo mobile technology

You've done it. Your wireless network is set up and your workforce is officially mobile. You've created a great tool for your business, but you may find that your computers don't allow you to take full advantage of it.

If you're ready to upgrade, consider investing in notebooks equipped with Intel® Centrino® Duo mobile technology. Our new dual-core processor is designed to empower a mobile workforce. Your employees will have greater connectivity options and better wireless performance[i] overall. Intel® Centrino® Duo mobile technology also enables greater battery life[1], and because of the dual-core processor, allows users to run more demanding applications simultaneously. So you'll find it's easier to multitask and to work remotely—even without a power source.

Intel® Centrino® Duo mobile technology can help you maximize the potential of your wireless network. It's the technology you need to be more efficient, more competitive, and more successful.

wireless checklist

1 System performance, battery life, high-definition quality and functionality, and wireless performance and functionality will vary depending on your specific operating system, hardware, and software configurations. References to enhanced performance as measured by SYSMark* 2004, PCMark* 2005, and 3DMark* 2005 refer to comparisons with previous generation Intel® Centrino® mobile technology platforms. References to improved battery life as measured by MobileMark* 2005, if applicable, refer to previous generation Intel Centrino mobile technology platforms. Wireless connectivity and some features may require you to purchase additional software, services, or external hardware. Availability of public wireless LAN access points is limited, wireless functionality may vary by country, and some hotspots may not support Linux-based Intel Centrino mobile technology systems. See www.intel.com/products/centrino/more_info for more information.

Copyright © 2006 Intel Corporation. All rights reserved. Intel, the Intel logo, Intel. Leap ahead. and Intel. Leap ahead. logo, Centrino and the Centrino logo are trademarks or registered trademarks of Intel Corporation or its subsidiaries in the United States and other countries.

* Other names and brands may be claimed as the property of their respective owners.

0206/ESW/STR/PP/10K 310744-001US